UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/650,440	08/27/2003	Frederic G. Thiele	END920030068US1	7247

26502   7590   11/14/2007
IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER
PERUNGAVOOR, VENKATANARAY

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
11/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

MAILED

NOV 1 4 2007

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/650,440
Filing Date: August 27, 2003
Appellant(s): THIELE ET AL.

Arthur Samodovitz(Reg. No. 31297)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/14/2007 appealing from the Office action

mailed 3/5/2007.

(1) Real Party in Interest

International Business Machines Corporation is the real party of interest.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2003/0145228 A1	SUURONEN ET AL.	07-2003
2002/0116512 A1	AMIT ET AL.	10-2002

| 6853619 | GRENOT | 2-2005 |
| 2002/0131369 A1 | HASEGAWA ET AL. | 09-2002 |

(9) Grounds of Rejection

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2,4-5, 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over

US Patent Publication 2003/0145228 A1 to Suuronen et al.(hereinafter Suuronen) in

view of US Patent Publication 2002/0116512 to Amit et al.(hereinafter Amit).

Regarding Claim 1, 13, Suuronen discloses the computer storage medium see Abstract;

first program to determine of packet is known exploit or portion thereof see Par. 0021; a

third program to determine administration packet see Fig. 1 item 20(IP packets that

cannot contain viruses, administration packets belong in this category). But fails to

explicitly disclose the packet being addressed to an broadcast address and further to

determine whether it is a new packet. However, Amit discloses the packet addressed to

a broadcast address see Fig. 4 item "Receiving TCP connection data" and further of

examining the packet to detect new packets see "Detect new connections requests".

Further yet, Amit discloses the new packets being classified as primary(i.e. known and reliable source, axiomatic to benign of instant invention) and secondary(unknown source) see "Classifying new connection request as "secondary"" & "Classifying new connection request as 'primary.'" It would be obvious to one having ordinary skill in the art at the time of the invention to include packet being addressed to an broadcast address and further to determine whether it is a new packet in the invention of Suuronen in order to be able to download new packets as taught in Amit see Par. 0035.

Regarding Claim 2, 14, 22, Suuronen discloses the firewall being used for scanning for via lotion of rules and determination of web traffic including webcrawlers and broadcast packets see Par. 0009 & Fig. 1. Suuronen discloses the dropping of packets from the Firewall(14) that do not comply with the rules, see Fig. 1. And packet being examined if the database can find it or otherwise considered new see Fig. 1 item 24.

Regarding Claim 4, 17, Suuronen discloses the blacklisting of packets so that known exploits can no longer have access to network's destination see Par. 0007.

Regarding Claim 5, 15, Suuronen discloses the gateway being used being several communication networks see Fig. 2-5, whereby the gateway is an computing device that is easily adaptable on an network and not a dedicated device.

Regarding Claim 7, Suuronen discloses the scanning of packets for signature see Fig. 1

item 22.

Regarding Claim 12, Suuronen discloses the packets being alerted when the packet is

not a broadcast or administration, known exploit see Fig. 1.

Regarding Claim 21, Suuronen discloses the computer storage medium see Abstract;

first program to determine of packet is known exploit or portion thereof see Par. 0021; a

third program to determine administration packet see Fig. 1 item 20(IP packets that

cannot contain viruses, administration packets belong in this category). But fails to

explicitly disclose the packet being addressed to an broadcast address and further to

analyzing the packets including protocols for valid protocols. However, Amit discloses

the packet addressed to a broadcast address see Fig. 4 item "Receiving TCP

connection data" and further of analyzing the packets including protocols for valid

protocols see Par. 0029. It would be obvious to one having ordinary skill in the art at the

time of the invention to include packet being addressed to an broadcast address and

further to determine whether it is a new packet in the invention of Suuronen in order to

be able to download new packets as taught in Amit see Par. 0034.

Claims 3, 8-11, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S

Patent Publication 2003/0145228 A1 to Suuronen et al.(hereinafter Suuronen) in view of

US Patent Publication 2002/0116512 to Amit et al.(hereinafter Amit) and further in view

of U.S. Patent 6853619 to Grenot.

Regarding Claim 3, Suuronen does not disclose the searching based on signature for

known exploits. However, Grenot discloses the searching based on signature for known

exploits see Col 6 Ln 8-25. It would be obvious to one having ordinary skill in the art at

the time of the invention to include the signature searching for known exploits in the

invention of Suuronen in order to search based on an quantitative measure as taught in

Col 8 Ln 48-52 of Grenot.

Regarding Claim 8, Suuronen does not disclose the examining of gateways and sub-net

masks. However, Grenot discloses the examining of gateways and sub-net masks see

Col 6 Ln 26-35.It would be obvious to one having ordinary skill in the art at the time of

the invention to include the examining of gateways and sub-net masks in the invention

of Suuronen in order to examining flows as taught in Grenot see Col 6 Ln 26-35.

Regarding Claim 9-11, 24, Suuronen does not disclose the comparing of IP addresses

and protocols. However, Grenot discloses the comparing of IP addresses and protocols

see Col 5 Ln 63-Col 6 Ln 3 & Col 3 Ln 13-23.It would be obvious to one having ordinary

skill in the art at the time of the invention to include the in the comparing of IP addresses

and protocols invention of Suuronen in order to have a first line of defense against an

attack.

Claims 6, 16, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S

Patent Publication 2003/0145228 A1 to Suuronen et al.(hereinafter Suuronen) in view of

US Patent Publication 2002/0116512 to Amit et al.(hereinafter Amit) further in view of

US Patent Publication 2002/0131369 A1 to Hasegawa et al.(hereinafter Hasegawa).

Regarding Claim 6, 16, 23, Suuronen does not disclose the administrator being alerted

and analysis result being reported. However, Hasegawa discloses the manager being

alerted and result being reported see Fig. 1 item 1, DB2.It would be obvious to one

having ordinary skill in the art at the time of the invention to include the manager being

alerted and result being reported in the invention of Suuronen in order to manager may

take an proactive approach to deal with the threat as taught in Hasegawa see Par.

0038-0043.

(10) Response to Argument

<u>Rejection of Claims 1, 4-5, 7, 12-13, 15 and 17 under 35 USC § 103 based on</u>

<u>Suuronen et al. and Amit et. al.</u>

The Appellant argues Claim 1 in this section of the Brief, namely the alleged absence of

certain features recited in Claim 1. And so, this claim is described in detail, relating to a

program instructions to determine if an new exploit is being identified. The Appellant

specifically argues the absence of details of second, third, fourth and fifth program

instructions of Claim 1. Accordingly, details of each program instructions are rebutted here.

Beginning with the second and third program instructions, the Appellant argues that Suuronen fails to disclose the second and third program instructions which determine if the packet is addressed to a broadcast IP address of a network or network administrative traffic. That is, a determination is made if the packet is sent to a network to be spread to everyone(i.e. broadcasted) or is an administrative traffic(i.e. relating to maintenance or administration of network). Suuronen discloses a gateway that filters the packets between two networks see Fig. 2 item 12, which gateway serves to spread the packet from the internet end to the LAN end(i.e. broadcast). The LAN end comprises many users that can receive the packets broadcasted from the common gateway. Further, Suuronen discloses the gateway can send packets to a particular destination after passing firewall see Par. 011(which can include many destinations, i.e. broadcasted).

The determination of a administrative traffic packet is also disclosed by Suuronen, albeit less explicitly, IP packet(first type) that can not contain viruses. Suuronen discloses an packet classification database used to compare incoming packet for types- first and second types see Fig. 1 item 16 & Par. 0021. The first type is known to be virus free and can be readily passed to the destination. The first type(Fig. 1 item 20) as classified by Suuronen contains information for setting up transmission session to other ports see

Par. 0019. And the setting up transmission to other ports is related to the network

administration function. Thus it apparent that the packet is an administration packet

used for network administration purposes.

Next, the Appellant argues that the fourth program instructions, the absence in

Suuronen of a determination of the packet being a not new(known) exploit candidate.

Suuronen discloses the screening of second type of packets against a virus detection

database see Fig. 1 item 24, for comparison with an known viruses. Further, Suuronen

discloses the database being updated with new data so that the database is able to

identify new and changing threats(i.e. viruses) see Par. 0021. And this done

dynamically, so that it is not a impose a burden on the system. The database functions

to identify the viruses that contained within the system.

Last, the Appellant argues that the fifth program instructions, the Suuronen nor Amit

reference being deficient of identification of a new exploit. Amit discloses the detecting

and classifying of request(i.e. data frames) see Fig. 2 item B. And this classification

further includes the packets, i.e. data being new or not see Fig. 4 item "Detect new

connection requests", further the new request are classified as primary and secondary

see Fig. 4 item "Classifying new connection request as 'primary'" & Classifying new

connection request as 'secondary'". The primary request is an familiar one from an

known entity(i.e. Internet) for loading a browser, while a secondary request is an

unfamiliar(i.e. outsider) used to complete download of web page components see Par.

0036 & Par. 0032. The secondary request is treated as a virtual connection as it cannot

be trusted see Fig. 5 item "Transferring 'virtual' requests to buffer" & Par. 0017. Amit

notes that the requests(i.e. packets) can be extended to messages from e-mail or chats

see Par. 0040.Thus the classification of packets into new primary or new secondary

packets satisfies the identification of new exploit as recited in the claim.

Even further, Suuronen discloses the identifying of known virus by comparing against a

database see Fig. 1 item 24. The mentioned database is updated with current

information regarding viruses see Fig. 1 item "Virus Updates", so this system is

dynamically suited to examine viruses. Extending this logic, viruses that can not be

identified are classified as a new exploit. That is, the database contains a complete

collection of viruses, if a virus can not be identified then it must be a new virus(i.e.

exploit).

And finally, the Appellant appears to argue the reason for combining, as it allegedly

relates to two different tasks. The Examiner disagrees, it is readily apparent that

Suuronen is concerned with network security through surveillance of packets see Fig. 1.

Similarily, Amit is concerned with surveillance of packets for security reasons see Par.

0002 & Par. 0007.

Rejection of Claims 2 and 14 under 35 USC § 103 based on Suuronen et al. and Amit et

al.

The Appellant appears to argue the same thing presented earlier, namely the absence

of an identification of a new exploit. Although this claim includes a web traffic crawler, it

apparent from the last section that the identification of a new exploit is disclosed by

Amit(see Par. 5 of Rejection of Claims 1, 4-5, 7, 12-13, 15 and 17 under 35 USC § 103

based on Suuronen et al. and Amit et. al.). With regard to the web traffic crawler newly

presented here, Suuronen discloses any packets being analyzed for different types of

attacks including port scanning, Denial-of-Service attacks see Par. 0021 & Par. 0010.

And it can be seen that the reference anticipates the web crawler traffic.

Rejection of Claim 9 under 35 USC § 103 based on Suuronen et al., Amit et al. and Grenot.

The Appellant appears to make the same arguments as before with the addition of

absence in Grenot of a determining of a protocol listed in a list of protocols assumed to

be harmless network broadcast traffic. The arguments relating to the determining of a

protocol listed in a list of protocols are rebutted here.

Grenot discloses a number of protocols to be used in determining a time reference and

communication, including Network Transport Protocol(NTP), Simple Network Time

Protocol(SNTP), Internet Protocol(IP) see Col 1 Ln 24-32 & Col 5 Ln 65- Col 6 Ln 3.

The named protocols are accepted at the destination end for processing of

frames/packets according to information sieved from the packets see Col 6 Ln 26-34.

This processing includes identification of packets and packet analysis see Col 8 Ln 27-52. The fact that the information can be gathered from the packet is itself an indication that the protocol has been understood(i.e. harmless) by the destination. That is, a packet contains information regarding ports, protocols, destination, source, among other things. If the destination is able to decipher the packet and extract the information after the packet analysis(signature/virus analysis), then this is positive proof of acceptance of the protocol as harmless.

The Appellant again argues the reason for combining Grenot with Suuronen and Amit, as it address different tasks and problems. As mentioned earlier, Suuronen and Amit are both concerned with surveillance of packets for viruses. Grenot like Suurnonen discloses the packet analysis, classification of packets and filtering based on classification see Fig. 3 item 42, 11 & 32. Thus the reason for combining is apparent to filter packets based on analysis(virus detection) and classification.

Rejection of Claims 3, 8, 10-11 and 24 under 35 USC § 103 based on Suuronen et al. and Grenot

The Appellant makes no new arguments in this section, but rather reiteriates the arguments present in a earlier section(see *Rejection of Claim 9 under 35 USC § 103 based on Suuronen et al., Amit et al. and Grenot)*, and so consult the named section for rebuttal.

Rejection of Claim 21 under 35 USC § 103 based on Suuronen et al. and Amit et al.

The Appellant makes no new arguments in this section, but rather reiteriates the arguments present in a earlier section(see *Rejection of Claim 9 under 35 USC § 103 based on Suuronen et al., Amit et al. and Grenot)*, and so consult the named section for rebuttal.

Rejection of Claim 22 under 35 USC § 103 based on Suuronen et al. and Amit et al.

The Appellant has already presented the arguments made in this section earlier in previous sections. And so, instead of restating the rejection, the Examiner intends to point out the section for rebuttal: arguments relating to broadcast, network administration traffic, and new exploit see *Rejection of Claims 1, 4-5, 7, 12-13, 15 and 17 under 35 USC § 103 based on Suuronen et al. and Amit et. al.*, arguments relating to web crawler traffic see *Rejection of Claims 2 and 14 under 35 USC § 103 based on Suuronen et al. and Amit et al.*, arguments relating to protocols listed in a list of protocols see *Rejection of Claim 9 under 35 USC § 103 based on Suuronen et al., Amit et al. and Grenot.*

Rejection of Claims 6, 16 under 35 USC 103 based on Suuronen et al., Amit et al., and

Hasegawa et al.

The Appellant makes no new arguments, but rather relies of Claim 1 for arguments. And accordingly, the rebuttal for this section is directed to that section see *Rejection of Claims 1, 4-5, 7, 12-13, 15 and 17 under 35 USC § 103 based on Suuronen et al. and Amit et. al.*

Rejection of Claims 23 under 35 USC 103 based on Suuronen et al., Amit et al., and Hasegawa et al.

The Appellant makes no new arguments, but rather relies of Claim 21 for arguments. And accordingly, the rebuttal for this section is directed to that section see *Rejection of Claim 21 under 35 USC § 103 based on Suuronen et al. and Amit et al.*
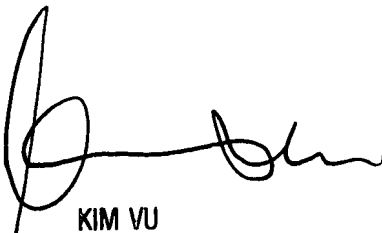
(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KIM VU
SUPERVISORY PATENT EXAM'
TECHNOLOGY CENTER 21^

/Venkat Perungavoor/

Venkat Perungavoor
Art Unit 2132
November 8, 2007

Conferees:

Kim Vu
SPE 2135

Hosuk Song